FinTech Australia

SUBMISSION PAPER:

CDR Privacy Safeguard Draft Guidelines

November 2019

This Submission Paper was prepared by FinTech Australia working with and on behalf of its Members; over 300 FinTech Startups, VCs, Accelerators and Incubators across Australia.

Table of Contents

About this Submission

This document was created by FinTech Australia in consultation with its Open Data Policy Working Group, which consists of over 150 company representatives. In particular, the submission has been compiled with the support of our Working Group Co-leads:

- Rebecca Schot-Guppy
- Alan Tsen

This Submission has also been formally endorsed by the following FinTech Australia members:

- Prospa
- Biza.io
- Banjo
- Credi
- Raiz
- Zip.co
- Brighte
- Frollo
- Harmoney Australia

Submission Process

In developing this submission, our Open Data Policy Working Group held a teleconference and circulated successive drafts of discussion points and a draft submission with members. This process canvassed key issues relating to the OAIC's CDR Privacy Safeguard Draft Guidelines.

We also particularly acknowledge the support and contribution of Cornwalls and DLA Piper to the topics explored in this submission.

Submission to the OAIC on the Draft Privacy Safeguard Guidelines

Fintech Australia is grateful for the opportunity to comment on the Draft Privacy Safeguard Guidelines released by the OAIC in October 2019.

Context: CDR in Australia

FinTech Australia has been a consistent advocate for policy reform to drive the implementation of a CDR framework in Australia. We have made numerous submissions to Federal Treasury, the Productivity Commission, the Open Banking Inquiry and Data 61 on the need for an Open Financial Data framework and on the details of that framework.

General Observations

We consider that the Guidelines are generally clear and helpful. We think that the overall structure, broadly aligned with the structure of the Australian Privacy Principle Guidelines, is appropriate and familiar to privacy practitioners and business alike.

We would however raise the point that the Guidelines are lengthy – and incorporate some complexity – including reaffirmed views as regards the OAIC's approach to the application of the Privacy Safeguards by reference to the Australian Privacy Principles (**APPs**). We do not believe this repetition is necessary (and may even lead to confusion), given that there are clear and accepted principles on the approach by the OAIC to its application and enforcement of the APPs (on which the Privacy Safeguards have been built / modelled). We would respectfully submit that the complexity and length of the Guidelines is likely to be detrimental to its intended purpose and we would recommend instead that the OAIC consider revising the Guidelines to focus only on those areas of exception to the approach taken by the OAIC to the Privacy Safeguards – i.e. CDR data will encompass by its very nature 'personal information' and although broader in scope, the current APPs and OAIC Guidelines will be applicable (in the vast majority of cases) to the handling of this information. The key exceptions being where CDR data involves that of (ii) a non-natural person (e.g. a company); and (ii) the categorisation of derived data. Although it is acknowledged that the Privacy Safeguards will generally apply instead of the APPs, the Safeguards are largely modelled on – and replicate – the core APPs – and so a consistent approach by the OAIC to the application and enforcement of similar terms should be

adopted.

The OAIC's approach on enforcing the Privacy Safeguards will surely be in the first instance informed and driven by its approach to enforcement of the APPs, and then only in the exception, will a novel approach be warranted in respect of the broader remit and obligations applicable to CDR data under the Privacy Safeguards. This would help promote more transparency for CDR consumers and active participants alike – as well as reduce the complexity and length of these Guidelines. Members are happy to provide further examples to the OAIC of their concerns in this regard.

Separately, and by way of general comment, we note that the Privacy Safeguards form part of and are enshrined in Part IVD of the Competition and Consumer Act **(CCA)** - an Act regulated by the ACCC. We welcome understanding whether the ACCC will be issuing similar guidelines on its approach to enforcement of the Privacy Safeguards with regard to serious and repeated breaches and as otherwise granted to the ACCC under the revised CCA. We recommend that the Guidelines are updated to make clear the role, remit and interaction of both regulators - and on the guidance issued by both regulators on their approach – and any cross-over (notwithstanding any general MoU which we note is intended to be put in place between the regulators).

Specific Submissions

1. *Protection of CDR Consumers who are not natural persons*

The Privacy Safeguards protect the CDR data of individuals and non-natural persons (e.g. companies) alike. We suggest the OAIC may wish to include a section under "Key Concepts" explaining the extent to which, if at all, separate policy and enforcement concerns will inform its role in relation to promoting compliance of the Privacy Safeguards in cases where the CDR consumer is not a natural person (e.g. it is a company). In particular, the approach taken to administering Privacy Safeguards 5, 6 and 7 may need to be calibrated according to whether the CDR consumer is, or is not, a natural person.

2. *Requirement to presume that a person is reasonably identifiable if it is unclear whether a person is in fact "reasonably identifiable"*

In Chapter B (Key Concepts), at B 33, the OAIC suggests that if it is unclear whether a person is "reasonably identifiable" (and therefore a CDR consumer) an entity should err on the side of

caution and act as though the person is 'reasonably identifiable' from the CDR data or other information held by the entity. This may be a reasonable and "safeguard friendly" approach to take, but we suggest that the OAIC monitor this issue during the testing phase. As an alternative to an entity having to make the presumption that a person is reasonably identifiable when that is in fact unclear, it may be more appropriate for the entity to conduct a risk assessment to make a reasonable decision about whether a person is, in fact, "reasonably identifiable". There are various methodologies available for these risk assessments, including those set out in the OAIC/Data 61 De-Identification Decision-Making Framework). In the alternate, our members would also be supportive of a removal from the OAIC guidelines of B33 in its entirety – given the scope possibly conflicting approaches and application – and to allow the existing guidance and market tests on what is meant by 'reasonably identifiable' under the Privacy Act regime to continue to apply.

3. Consents from CDR Consumers who are not natural persons

Under Chapter C (Consent) at C 18, the OAIC suggests that where a consumer is not a natural person (e.g. it is a company) the accredited person should ensure that the consent is given by a person who is duly authorised to provide the consent on the entity's behalf. This principle is correct. But in light of the difficulties in making the Corporations Act assumptions of due execution where a document is obtained from a CDR consumer through an online process, it would be helpful for accredited persons to have (non-prescriptive) additional guidance about what the OAIC will generally accept as a valid online consent from a non-natural person, such as a company.

4. Present coverage of the CDR Regime

In Chapter C (Consent) at C 18, OAIC suggests that "the CDR regime currently extends only to business accounts in an individual's name". This suggestion does not seem to be consistent with Part 2 of Schedule 3 of the CDR Rules. As noted in paragraph B52 of the Guidelines, a consumer in the banking sector is "eligible" if they have an account with the data holder that is open and set up in such a way that it can be accessed online. This is not limited to individuals.

5. Boxed comment under paragraph 2.13 (Privacy Safeguard 2)

6. Written note of a use or disclosure (Privacy Safeguard 6)

In Chapter 6 (Privacy Safeguard 6), OAIC suggests that the requirement to make a written note of a use or disclosure should include the following details:

- The date of the use or disclosure
- Details of the CDR data that was used or disclosed
- The relevant Australian law or tribunal or court order that required or authorised the use or disclosure
- If the accredited recipient used the CDR data, how the CDR data was used by the accredited data recipient
- To whom the CDR data has been disclosed, if applicable.

We suggest that these requirements should take effect "to the extent that is reasonably practicable". In some circumstances it may be onerous and impractical for a note to be made of all of the above details, and we suggest that a generic record of use or disclosure should suffice instead.

7. Liability of accredited data recipients under section 56EK(2) of the CCA

Paragraph 8.2 includes a general statement that where an accredited data recipient takes reasonable steps to ensure that the overseas recipient does not breach the Privacy Safeguards, but the overseas recipient nonetheless contravenes a relevant privacy safeguard, the accredited data recipient is accountable for that contravention, notwithstanding the fact that they complied with their Privacy Safeguard 8 obligations. We suggest that this general statement in paragraph 8.2 should be qualified by cross referencing the matters set out in paragraph 8.41, which reflect section 56EK(2)(b) of the CCA. That is, the accredited data recipient is accountable for the contravention of the overseas recipient if:

- the overseas recipient is not an accredited person,
- the accredited person does not reasonably believe that the overseas recipient is bound by a law or scheme that is similar to the CDR regime and that a consumer will be able to enforce protections provided by that law or scheme; or
- the conditions specified in the consumer data rules are not met.

Other comments

While recognizing that it may not strictly be within the scope of the subject matter of this submission, we understand that the current CDR technical specifications effectively only allow a single sharing agreement to be established between a single CDR consumer/accredited data recipient/data holder triplet. As a result, when a new sharing agreement is established for that

triplet, it effectively replaces - or “overwrites” - any prior data sharing agreement for that particular triplet. The impact of this limitation could manifest itself in a number of ways relevant to the discussion in Chapter C of the Guidelines. For example:

- despite the availability of a dashboard, a CDR consumer may consent to additional access without realising that this modifies an existing consent granted previously in an agreement for that triplet- this is likely to not only be confusing to the CDR consumer but ultimately to increase the amount of friction the CDR consumer must endure to have a continuous relationship with the accredited data recipient;
- despite the data minimisation principle, an accredited data recipient may seek to request access to more data than initially necessary on the basis that by doing so they will have the necessary data available should a CDR consumer choose to use an optional feature within the accredited data recipient's product;
- it has been suggested to us that because the consent agreement is not immutable (as it can be replaced, in-line), there may be flow on impacts to the audit and compliance obligations of both data holders and accredited data recipients alike. Further, it is possible that regulators will encounter challenges when performing retrospective compliance verification activities as data sharing agreements can encounter potentially invisible state changes;
- accredited data recipients may have challenges adhering to rules governing data deletion as the original consent for information may not be aligned to the end state of a new consent. This represents a potential processing issue requiring additional compliance controls by all parties; and
- if a finer set of consent controls are introduced at a later time (and here we reference the distinction between “fine grained” and “coarse-grained authorisations at paragraph 9.6 of the ACCC’s Consumer Data Rights Rules Framework) this will potentially exacerbate the above issues as it could result in consent agreements for one set of accounts/functions governing a particular CDR consumer/data holder/accredited data recipient triplet overwriting those for a separate set of accounts/functions between the members of that triplet.

Conclusion

We appreciate the opportunity to make this submission. We would be pleased to discuss any aspect of this submission with the OAIC.

About FinTech Australia

FinTech Australia is the peak industry body for the Australian fintech Industry, representing over 300 fintech Startups, Hubs, Accelerators and Venture Capital Funds across the nation.

Our vision is to make Australia one of the world’s leading markets for fintech innovation and

investment. This submission has been compiled by FinTech Australia and its members in an effort to drive cultural, policy and regulatory change toward realising this vision.

FinTech Australia would like to recognise the support of our Policy Partners, who provide guidance to the association and its members in the development of our submissions:

- DLA Piper
- Hall & Wilcox
- King & Wood Mallesons
- K&L Gates
- The Fold Legal
- Cornwalls
- Baker McKenzie